Completed Alert Ticket

Ticket ID: A-2703

Alert Message: SERVER-MAIL Phishing Attempt - Possible Malware Download

Severity: Medium

Details: A user may have interacted with a phishing email by opening attachments or clicking links.

Ticket Status: Escalated

Ticket Comments:

The alert flagged that an employee downloaded and opened a malicious file from a phishing email. There is a notable discrepancy between the sender's email address "76tguy6hh6tg@rt7tg.su," the email body name "Clyde West," and the sender's name "Def Communications." Additionally, the email's subject line and body contained grammatical errors. The body also included a password-protected attachment titled "bfsvc.exe," which was downloaded and executed on the affected system. Based on previous analysis, the file hash has been confirmed as malicious. Due to these findings, I escalated this ticket to a level-two SOC analyst for further action.

Additional Information:

- Known Malicious File Hash: 54e6ea47eb04634d3e87fd7787e2136cc6cc80ade34f246a12cf93bab527f6b

Email Details:

From: Def Communications <76tguy6hh6tg@rt7tg.su> [114.114.114.114]

Sent: Wednesday, July 20, 2022, 09:30:14 AM

To: <hr@inergy.com> [176.157.125.93]

Subject: Re: Infrastructure Engineer Role

Email Body:

Dear HR at Ingergy,

I am writing to express my interest in the engineer role posted on your website.

Attached are my resume and cover letter. For security reasons, the file is password protected.

Please use the password paradise10789 to open it.

Thank you,

Clyde West

Attachment: bfsvc.exe